(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 776 445**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **98 03242**

(51) Int Cl[6] : **H 04 L 9/20**

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 17.03.98.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 24.09.99 Bulletin 99/38.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *SCHLUMBERGER INDUSTRIES SA Société anonyme* — FR.

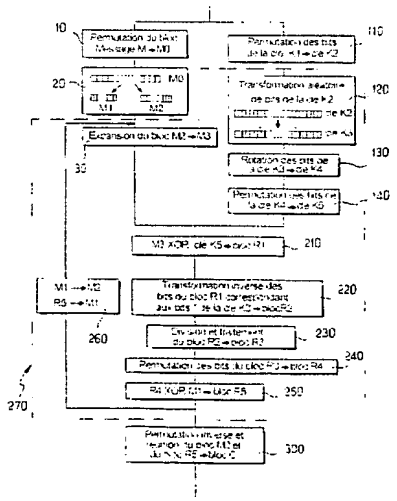
(72) **Inventeur(s) :** SALLE PATRICK.

(73) **Titulaire(s) :**

(74) **Mandataire(s) :** PATCO SA.

(54) PROCEDE DE SECURISATION DE DONNEES METTANT EN OEUVRE UN ALGORITHME CRYPTOGRAPHIQUE.

(57) L'invention concerne un procédé de sécurisation de données mettant en oeuvre un algorithme cryptographique comprenant au moins un cycle d'exécution d'opérations répétitives de traitement d'éléments de données (K2, RI) pour élaborer une information chiffrée (C), ce procédé comprenant au moins une étape (120, 220) de modification aléatoire de l'exécution d'au moins une opération d'un cycle à un autre ou d'au moins un des éléments de données de telle sorte que l'information chiffrée soit inchangée par cette modification aléatoire.



FR 2 776 445 - A1

La présente invention concerne un procédé de sécurisation de données, destiné par exemple à être mis en oeuvre par le microprocesseur d'une carte bancaire ou une carte d'autorisation d'accès lors d'une connexion à un terminal informatique d'authentification.

Les procédés de sécurisation de données de type connu mettent en oeuvre un algorithme cryptographique comprenant des cycles d'exécution d'opérations répétitives de traitement d'éléments de données contenus dans une mémoire de la carte pour élaborer une information chiffrée destinée à être communiquée au terminal informatique.

L'exécution du procédé par le microprocesseur de la carte engendre l'émission de signaux dérivés tels que des pics de consommation au niveau de l'alimentation électrique du microprocesseur, ou des variations du rayonnement électromagnétique de sorte que l'enveloppe du rayonnement électromagnétique est significative des données traitées. Un fraudeur désirant utiliser de façon non autorisée les cartes à microprocesseur peut lancer à plusieurs reprises l'exécution du procédé et analyser les signaux dérivés émis pour établir des correspondances entre les différentes opérations de traitement et chaque signal ou série de signaux. A partir de ces correspondances, et en soumettant par exemple la carte à des perturbations électromagnétiques ou des baisses de tension à des instants précis du déroulement de l'algorithme, le fraudeur peut étudier l'information chiffrée obtenue et les différences, ou au contraire l'absence de différences, entre les signaux dérivés émis pour découvrir les données contenues dans la mémoire de la carte.

Pour compliquer une telle analyse des signaux dérivés, on a pensé à engendrer des signaux parasites venant s'ajouter aux signaux dérivés émis lors de l'exécution du procédé. L'extraction des signaux correspondant à l'exécution du procédé est alors plus délicate mais demeure

possible. On a également pensé à concevoir les composants électroniques de la carte et le programme d'exécution du procédé de sorte que les signaux dérivés émis soient indépendants de la valeur des données sensibles. Toutefois, ceci complique la réalisation des cartes sans assurer une protection satisfaisante des données.

Un but de l'invention est de proposer un procédé de sécurisation efficace ne présentant pas les inconvénients précités.

En vue de la réalisation de ce but, on prévoit, selon l'invention, un procédé de sécurisation de données mettant en oeuvre un algorithme cryptographique comprenant au moins un cycle d'exécution d'opérations répétitives de traitement d'éléments de données pour élaborer une information chiffrée, ce procédé comprenant au moins une étape de modification aléatoire de l'exécution d'au moins une opération d'un cycle à un autre ou d'au moins un des éléments de données de telle sorte que l'information chiffrée soit inchangée par cette modification aléatoire.

Par modification aléatoire de l'exécution d'au moins une opération, on entend une modification de l'ordre d'exécution d'opérations ou de parties d'opérations, ou une modification du déroulement d'une seule opération. Ainsi, au moins une opération et/ou au moins une des données traitées sont modifiées aléatoirement, ce qui affecte de façon aléatoire les signaux dérivés émis. Il est de ce fait très difficile pour un fraudeur de distinguer les différentes opérations de traitement et de découvrir les données à partir des signaux dérivés. En outre, la modification aléatoire n'affecte pas l'information chiffrée de sorte que celle-ci peut être utilisée de façon habituelle après son élaboration.

D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description qui suit d'un mode de mise en oeuvre particulier non limitatif

de l'invention, en relation avec la figure unique annexée illustrant sous forme d'un schéma par blocs le déroulement du procédé selon ce mode de mise en oeuvre.

Le procédé de sécurisation selon l'invention est ici décrit mettant en oeuvre un algorithme cryptographique de type DES (abréviation des termes DATA ENCRYPTION STANDARD) en vue d'élaborer une information chiffrée C de 64 bits à partir d'un bloc message M et d'une clé secrète K1 eux-mêmes de 64 bits.

Le procédé débute par la permutation 10 des bits du bloc message M entre eux pour former le bloc M0.

Le bloc M0 est alors divisé en deux blocs M1 et M2 de 32 bits lors d'une étape de division 20.

Il est ensuite procédé à l'expansion 30 du bloc M2 pour former un bloc M3 de 48 bits. Cette expansion 30 est par exemple réalisée en découpant le bloc M2 en huit quartets et en ajoutant à chaque quartet le bit extrême adjacent des quartets encadrant le quartet concerné (les quartets extrêmes étant considérés comme adjacentes).

Parallèlement à ces opérations, une permutation 110 est effectuée sur les bits de la clé K1 pour former la clé K2. Les bits non significatifs de la clé K1 sont simultanément supprimés de sorte que la clé K2 a seulement 56 bits.

Selon l'invention, les bits de la clé K2 sont alors modifiés aléatoirement lors d'une transformation 120. Les bits de la clé K3 correspondant aux bits modifiés de la clé K2, ici marqués par une étoile, sont mémorisés. La transformation aléatoire 120 est par exemple réalisée en associant à la clé K2, par l'intermédiaire d'un opérateur logique de type OU exclusif, un nombre aléatoire engendré par un générateur de nombres non prédictibles de la carte.

Une clé K4 est obtenue par la rotation 130 des bits de la clé K3. Puis, une permutation 140 est réalisée sur les bits de la clé K4 pour former la clé K5. Simultané-

ment à la permutation 140, les bits non significatifs de la clé K4 sont éliminés de sorte que la clé K5 comporte 48 bits.

Le procédé se poursuit par l'association 210 du bloc M3 et de la clé K5 par l'intermédiaire d'un opérateur logique de type OU exclusif. Le résultat de cette association est le bloc R1.

La transformation inverse des bits du bloc R1 correspondant aux bits modifiés par la transformation 120 est ensuite réalisée pour former le bloc R2. Cette transformation 220 inverse de la transformation 120 vise à remettre les bits du bloc R1 correspondant aux bits marqués d'une étoile dans l'état dans lequel ils auraient été en l'absence de la transformation 120.

Il est ensuite procédé, de façon classique, à la division et au traitement 230 du bloc R2, à la permutation 240 des bits du bloc R3 formés lors de l'étape 230, et à l'association 250 du bloc R4 résultat de l'étape 240 au bloc M1 par un opérateur OU exclusif pour former le bloc R5.

Le groupe d'opérations, désigné de manière générale par la référence 270, est ensuite exécuté à nouveau à quinze reprises en affectant, à chacune de celles-ci, la valeur du bloc M1 au bloc M2 et la valeur du bloc R5 au bloc M1 lors d'une étape d'affectation 260.

Le procédé se termine par l'opération 300 d'obtention de l'information chiffrée C par la permutation inverse et la réunion du bloc dernier M2 et du bloc dernier R5 obtenus.

On comprend que l'étape de modification aléatoire de la clé K2 comprend la phase de transformation 120 et la phase de transformation inverse 220. Ces deux phases permettent d'obtenir une information chiffrée C qui n'est pas affectée par cette modification aléatoire.

On pourrait également réaliser de la même manière

une modification aléatoire du bloc M2 et/ou d'une autre donnée.

Selon un autre mode de mise en oeuvre de l'invention, lequel peut être associé à une étape de modification telle que précédemment décrite, l'exécution d'au moins une opération peut être modifiée de façon aléatoire d'un cycle à l'autre, un cycle pouvant être un cycle complet d'exécution de l'algorithme ou un cycle intermédiaire d'exécution d'un groupe d'opérations.

Par exemple, une détermination aléatoire de l'ordre d'exécution de certaines opérations peut être réalisée au cours d'un cycle d'exécution de l'algorithme. Les opérations retenues seront celles dont l'ordre d'exécution les unes par rapport aux autres n'influent pas sur le résultat. Pour réaliser cette détermination, on pourra prévoir à la fin des opérations choisies un saut conditionnel vers certaines opérations en fonction de la valeur d'un nombre aléatoire ou définir un tableau des adresses des différentes opérations parcouru de façon aléatoire.

A titre d'exemple, la permutation 10 des bits du bloc message M pourrait être effectuée après la permutation 110 des bits de la clé K1 ou inversement.

De même, il pourrait être prévu une détermination aléatoire de l'ordre d'exécution des opérations du groupe 270 pour chaque cycle intermédiaire d'exécution de celles-ci (16 cycles intermédiaires d'exécution de ces opérations pour un cycle complet d'exécution de l'algorithme). Là encore, l'ordre d'exécution de ces opérations sera choisi pour ne pas influer sur le résultat.

Par ailleurs, pour certaines opérations, les données sont traitées par éléments. Ainsi, lors de l'expansion 30, les blocs M2 sont traités par quartets. Lors de cette opération, on peut prévoir de déterminer aléatoirement l'ordre de traitement des différents quartets. De même, lors de la permutation 140 les bits de la clé K4 sont

traités individuellement. Une étape de détermination aléatoire de l'ordre de traitement des bits peut également être prévue pour l'exécution de cette permutation. Les quartets du bloc M2 peuvent également être traités en alternance avec les bits de la clé K4, c'est-à-dire que l'on traite par exemple un premier quartet du bloc M2 puis une série de bits de la clé K4, puis un deuxième quartet du bloc M2 etc., en mémorisant à chaque fois les éléments de donnée traités afin de contrôler que toutes les opérations requises sont bien exécutées.

Bien entendu, l'invention n'est pas limitée au mode de réalisation qui vient d'être décrit, mais englobe au contraire toute variante reprenant, avec des moyens équivalents, ses caractéristiques essentielles.

En particulier, bien que l'invention ait été décrite en relation avec un algorithme de type DES, l'invention peut être appliquée à d'autres algorithmes cryptographiques tels que l'algorithme RSA (abréviation du nom de ses auteurs Riverst, Shamir , Adelman) ou l'algorithme dit de Fiat Shamir.

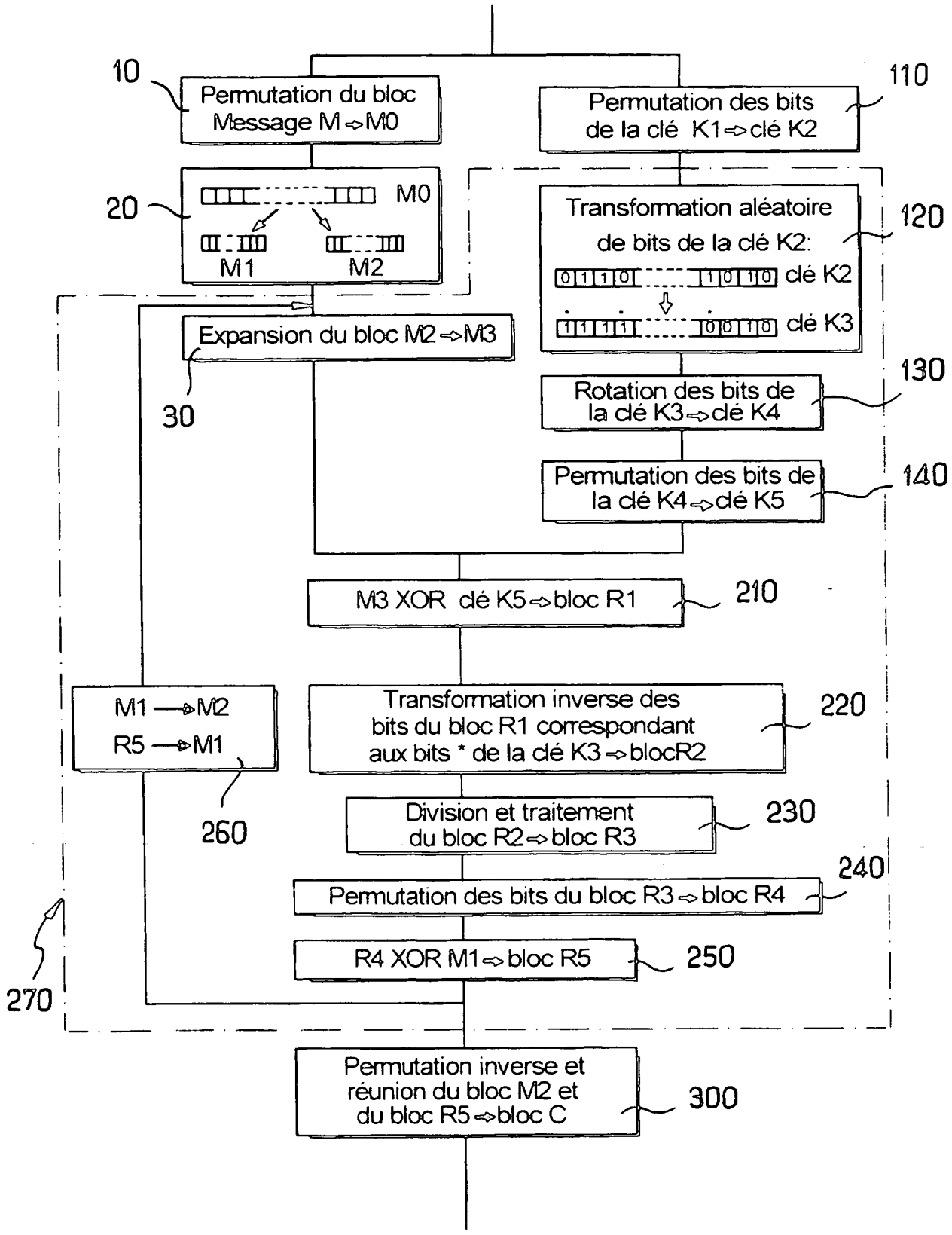
Par ailleurs, les nombres de bits des données ne sont mentionnés qu'à titre indicatif et peuvent être modifiés pour être adaptés au degré de sécurisation envisagé.

REVENDICATIONS

1. Procédé de sécurisation de données mettant en oeuvre un algorithme cryptographique comprenant au moins un cycle d'exécution d'opérations répétitives de traitement d'éléments de données (K2, R1) pour élaborer une information chiffrée (C), caractérisé en ce qu'il comprend au moins une étape (120, 220) de modification aléatoire de l'exécution d'au moins une opération d'un cycle à un autre ou d'au moins un des éléments de données de telle sorte que l'information chiffrée soit inchangée par cette modification aléatoire.

2. Procédé de sécurisation selon la revendication 1, caractérisé en ce que l'étape de modification aléatoire comprend le traitement dans un ordre aléatoire de bits ou de groupes de bits d'au moins un élément de donnée.

3. Procédé de sécurisation selon la revendication 1 ou la revendication 2, caractérisé en ce que l'étape de modification aléatoire comprend une phase (120) de transformation aléatoire d'éléments d'au moins une donnée, et, postérieurement à au moins une opération (130, 140, 210) de traitement de cette donnée, une phase (220) de transformation inverse des éléments de la donnée traitée correspondant aux éléments préalablement transformés.



REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

2776445

N° d'enregistrement national

FA 560304
FR 9803242

DOCUMENTS CONSIDERES COMME PERTINENTS

Categorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendications concernees de la demande examinée
X	KOCHER P C: "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems" ADVANCES IN CRYPTOLOGY - CRYPTO'96. 16TH ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE. PROCEEDINGS, SANTA BARBARA, CA, USA, 18-22 AUG. 1996, pages 104-113, XP000626590 ISBN 3-540-61512-1. 1996, Berlin, Germany, Springer-Verlag, Germany * abrégé * * page 111, ligne 23 - dernière ligne * * page 112, alinéa 3 *	1,3

DOMAINES TECHNIQUES RECHERCHES (Int.CL.6)

H04L

1

Date d'achèvement de la recherche	Examinateur
4 décembre 1998	Holper, G

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique general
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)